Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 4, Issue. 1, January 2015, pg.403 – 407

RESEARCH ARTICLE

Development of a Secure Mail Client

Saritha P, Nitty Sarah Alex

Software Engineering, India

Software Engineering, India

sarithap024@gmail.com; nittyalex82@yahoo.co.in

***Abstract*- The importance and usage of internet and email correspondence have shown tremendous advancement during past two decades. Recently, email has emerged as one of the exploited features of internet which made the security of transmitted information as one of the essential requirement. This paper involves the development of a secure mail client which would facilitate confidentiality, authenticity and message integrity achieved through the use of cryptographic systems ensuring the users with security and privacy.**

Keywords: Two factor authentication, Sieve, Recaptcha, S/mime.

I. INTRODUCTION

The worldwide scope of internet has allowed its users the opportunity to access enormous amounts of information and provide straightforward means to interact and collaborate. Today, email is one of the most commonly used network application. Mails are retrieved through email clients. An email client is a computer program which is used to manage a user's mail. A mail server also known as mail transfer agent (MTA) which is an application that receives email from local users and forward outgoing mail for delivery. Typically, email client requires an email address to be setup and configured before user can start using email service. One of the critical problem observed in mail clients is its security. Also the email messages send across the internet is not protected as it could be misdelivered or read by unauthorized individuals. Currently all mail clients provide authentication through a username and password which is vulnerable to attacks as the passwords could be easily hacked. Thus it became necessary to provide with extended security or authentication feature as the two factor authentication which uses several factors like what you know, what you have or what you are.

II. RELATED WORKS

Email systems are based on client server architecture and message is send from any clients to a central server. This central server reroute mail to its intended destination. The first "real" email was found by Ray Tomlinson of the now defunct ARPANET network, which in 1971 sent out a message which he received seconds later, on a computer placed next to the first one. The first email client program ever developed was named MSG. At the beginning, email was sent through a FTP(File Transport Protocol)-like structure. MSG was also one of the basis in creating the SMTP (Simple Mail Transfer Protocol)-type server, which is now the standard gate through all or our messages pass in order to reach their email clients. One of the first email clients that offered the user with a text interface was Elm. Email has evolved into communication tool of choice for IT ,academics and professional. Initially it was developed only based on text as shown in Fig 1. Basically there are four types of mail clients. They are Linux and unix email clients, Mac email clients, Web based email clients and Windows email clients. The disadvantage of using webmails is that it has to be always connected to internet for the users to view their mails. Windows email clients offer to share connection with people since it can be configured for use by a number of people. Email clients can help people to manage their messages quickly and also they are not bound exclusively to use their own personal computers. Some of the limitations of earlier email clients were that:

- It could send only text files[1] and even though user could send images, programs and files like Ms word, some users was not able to use it.
- Other problem was lack of context support or limited context for which the users would require a dynamic way to connect related messages.
- Most of the email clients are based on single username and password. This authentication is considered to be unsafe as the hacker could easily get the password through dictionary method.
- Protection of mailboxes is other major issue. As the mail letters on servers depend on operating system and if the operating system is not properly configured hackers could easily attack the mailbox.
- Spam and phishing[2] is considered to be other major issue which exploits the authorization of email standards thus resulting in anyone sending email to any other user.
- The other issue is the email spoofing which happens something like an email claiming to be from system admin requesting users to change password to a specified string and threatening to suspend their account if they do not do so.
- Address book provided by email systems which is stored on the workstation is very clear and thus could be hacked or stolen by any intruder.

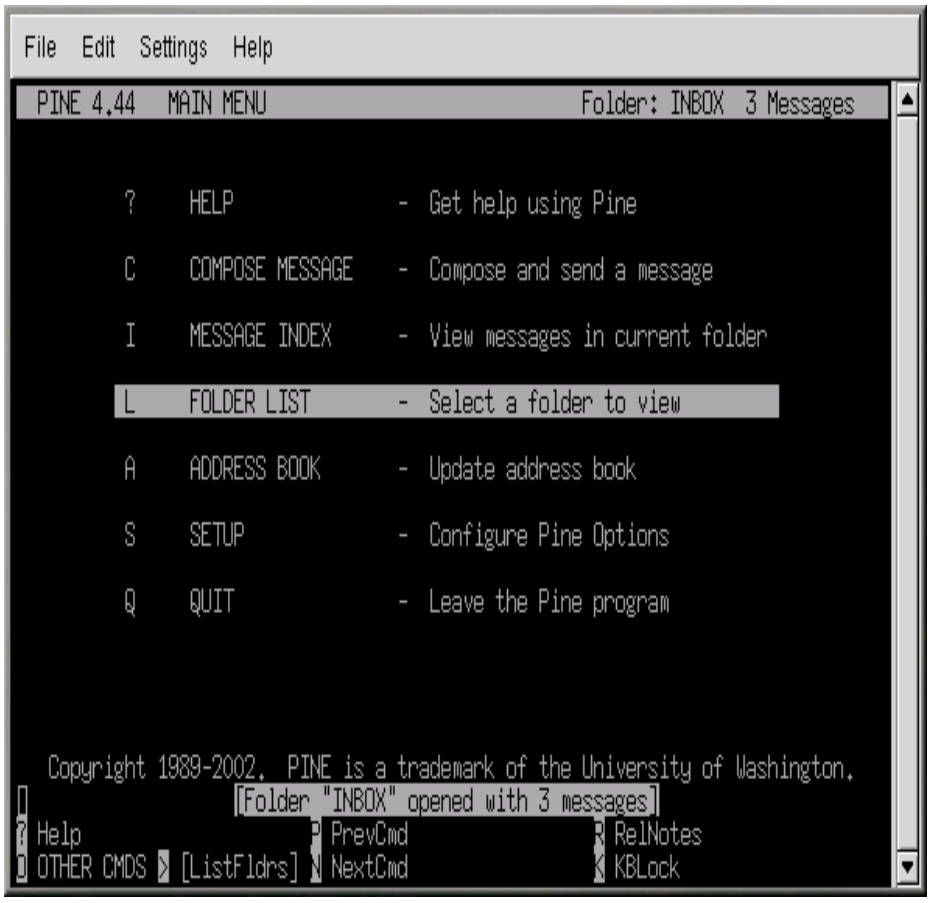

Fig 1

From past there has been various methods used to make emails secure[3]. First of this was the Privacy Enhanced Mail(PEM).This had two main protection features which were the signed messages and the encrypted messages .The details of PEM[4,5] are described in four internet RFC's as RFC 1421 describes message encryption and authorization,RFC1422 describes certificate based key management, RFC 1423 describes message and integrity algorithms. Users publish their RSA key in digital certificates which itself were signed using RSA of a certifying authority which in turn is signed by other certifying authority thus forming a certificate chain leading back to the single trusted user. Because management of a single user was problematic S/MIME[6](secure Multipurpose Mail Extensions) came into existence. Here the S/MIME messages appear as ordinary messages with an additional attachment name smime.p7s.Next was the Pretty Good Policy(PGP).The difference between PGP and PEM was that PEM specified a centralized Public Key Infrastructure(PKI) with a single root whereas PGP users can independently certify keys as belonging to other users. PGP is mainly used to encrypt a message or file so that only receive could decrypt it, clearly signaling the text message guaranteeing to have come from the intended sender and not the intruder. As PGP did not come with licences it was like a separate program which did not transparently interoperate with the existing mail clients.

III. PROPOSED SYSTEM

The proposed system is to develop a secure mail client which will have minimal features of a mail client and would provide two factor authentication[7] rather than single username and password. Use of jsp pages compiles to full java servlet unlike any client –server script which avoids the parsing and interpretation each time.

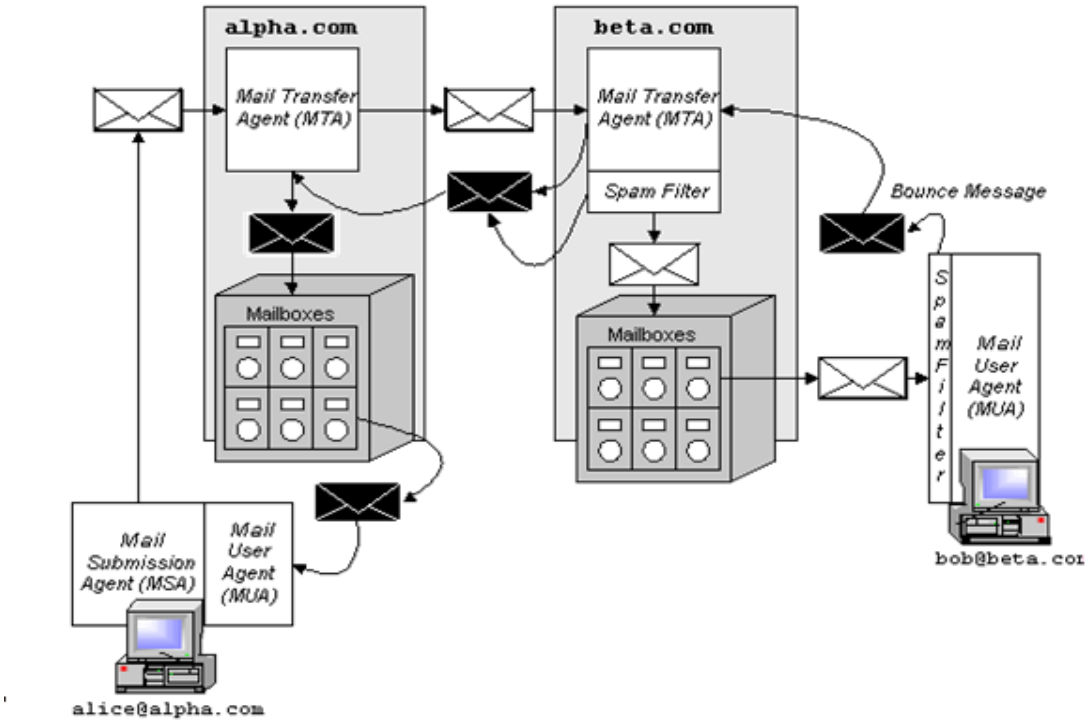

Fig 2

The system is intended to use Cyrus IMAP which performs better than maildir as it allows mail filtering through the implementation of mail filtering language called sieve. Two factor authentication is provided through the session pin. A session pin is generated post validation of username – password and CAPTCHA which is based on time synchronization between client and server providing session. Here CAPTCHA used is the RECAPTCHA. RECAPTCHA provides the images of words which would not be able to be read by optical character recognition software thus preventing bots or other software agent from using the account. It uses random sequence generation algorithm to generate a new password. The proposed system also provides custom security at different levels of management. The user's position in an organization is a key field entered in database maintenance. Additional security is provided depending on the designation of the users in an organization varying from regular employees to managers to higher positions. Also SSL/TLS would provide options for authenticating mechanisms. Encryption and hashing algorithm is used for secure transfer of mail. The user's account is provided with set of features such as composing, sending of email and folder management. Mail exchanged across networks will be passed between mail servers that run on specially designed software. To enter the server, email must go through a sieve which acts as a filter for span type mail. Mail Transfer Agent will identify the correct recipient mailbox and update the receiver account. Thus the system is considered to have three modules which is the front end application, server configuration and custom security. Front end application is where the user enters username and password along with CAPTCHA and session pin. Server configuration is concerned with the mailbox features and spam filters which helps in filtering of unwanted messages as shown in the Fig 2.Security is provided by two factor authentication which is provided immediately after the Captcha verification. A one time password is created by a random 8 digit pin which is generated by the server making use of secure random property of java security package for which a GSM modem has to be integrated to the mail client. Also security is provide through SSL handshake for encrypting the information between client and servers. The other module considered is the customized security which is

specially provided for the mail clients developed for any organization. When employees are accessing their account from within the organization they are exempted from entering session pin as they are accessing it from trusted ip. Role of an employee can constitute a layered pattern .Sessions would be based on their role. When higher authority wants to access their mail they are restricted to do so only through their system. This could be achieved through MAC address matching. By doing this though the intruder might know the username and password he will not be able to access as there would be a warning send to the concerned employee.

IV. CONCLUSION

The paper discusses about the development of a secure mail client which has the minimal features of a mail client and also provides a two factor authentication based on session pin generation. This is provided by using hash algorithm and random pin generation algorithm. Thus it is more secure than the existing mail clients which has only a single username and password authentication. As a future enhancement extra security feature other than using PGP or S/mime can be provided by creating a proxy server[8] which could be placed in between the email client and the email server. In this the email client either generates self-signed certificates or requests it from the Certifying Authority. Server also generates a self-signed certificates or requests from Certifying Authority. A connection will be initiated only if the certificates could match each other thereby ensuring security.

REFERENCES

[1] Xing Hu,Development Of Textual Email Clients in java,University of Bath(2005)

[2] Federal Trade Comission. Identity thief goes “phishing” for consumers’ credit information, July 2003.

[3] Simson L. Garfinkel, David Margrave, Jeffrey I. Schiller, How to Make Secure Email Easier To Use

[4] J. Linn. RFC 1421: Privacy enhancement for Internet electronic mail: Part I: Message encryption and authentication procedures, February 1993.Obsoletes RFC1113.

[5] S.Kent,RFC 1422,Privacy enhancement for electronic mail: Part II :Certificate based key management, February 1993.Obsoletes RFC1114

[6] B.Ramsdell RFC3851: Secure or multipurpose internet mail extensions(s/mime) version 3.1 message specification,july 2004.

[7] NETWORK WORLD The Connected Enterprise ,May 20,2013, Two Factor Authentication Home.

[8] CryptoNet: Design and Implementation of the Secure Email System .Abdul Ghafooor, Sead Muftic and Gernot Schmolzer NUST school of Electrical Engineering and Computer Science,Sector H-12,Islamabad, Pakistan.

